

**Department of Defense****Global Networked Information Enterprise Information Assurance Policy**

March 1, 1999

ASD (C3I)

**Part I – Policy and Responsibilities****1. PURPOSE:** This policy memorandum:

1.1. Supplements DoD Directive 5200.28, DoD Manual 5200.28-M, and DoD Directive C-5200.5 (references (a), (b), and (c)) and establishes policy and assigns responsibilities for information assurance (IA) of the DoD Global Networked Information Enterprise (GNIE)

1.2. Establishes information system mission categories and levels of protection.

**2. APPLICABILITY AND SCOPE:**

2.1. This policy memorandum applies to:

2.1.1. The Office of the Secretary of Defense; the Military Departments and their respective Services; the Chairman of the Joint Chiefs of Staff and the Joint Staff; the Unified Combatant Commands; the Inspector General of the Department of Defense; the Defense Agencies and DoD field activities (hereafter referred to collectively as "DoD Components").

2.1.2. All information system technologies that are used to enter, process, store, display or transmit DoD information within the GNIE, regardless of classification or sensitivity.

2.3. This policy memorandum does not address additional measures that may be required for the protection of foreign intelligence or counterintelligence information, Sensitive Compartmented Information (SCI) (reference (d)), Single Integrated Operating Plan – Extremely Sensitive Information (SIOP-ESI) (reference (e)), or Special Access Program (SAP) information (reference (f)) that transit the GNIE.

**3. DEFINITIONS:**

3.1. Terms used in this policy memorandum are defined in National Security Telecommunications and Information Systems security Instruction (NSTISSI) No. 4009 (reference (g)) or Part IV.

4. POLICY: It is DoD policy that:

4.1. All DoD information and resources shall be appropriately safeguarded at all times in order to support defense in depth across the DoD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based on mission criticality, level of required information assurance and classification or sensitivity level of information entered, processed, stored, displayed, or transmitted.

4.2. All DoD systems within the GNIE shall be assigned to a mission category (mission critical, mission support or administrative) that reflects the type of the information handled (i.e., entered, processed, stored, displayed, or transmitted) by the system relative to the achievement of DoD goals and objectives. Mission categories will be determined by the DoD functional domain owner (e.g., logistics, transportation, medical, intelligence, personnel, financial) or the responsible DoD Component head, in consultation with the information owner. System mission categories, functional domain, and mission owner are defined in Part IV.

4.3. All systems shall be employed with protection mechanisms, intrusion detection capabilities, reporting mechanisms, and provisions for recovery and continuity of operations consistent with the functional domain and DoD Component mission functions they perform and shall be configured, managed and operated to achieve the appropriate levels of protection as specified in Part II.

4.4. Resources sufficient to ensure compliance with this policy memorandum shall be planned, budgeted, allocated and executed.

4.5. Information assurance shall be managed to ensure that the principles contained in this policy memorandum are included in the decision-making processes throughout the entire life cycle of all systems within the GNIE in accordance with DoD Regulation 5200.1R (reference (h)).

4.6. Only National Security Agency (NSA) certified cryptographic modules shall be employed in products used to encrypt classified information or sensitive information delineated by Title 10, United States Code, Section 2315 (reference (i)).

4.7. Sensitive information subject to Public Law 100-235 (reference (j)) shall be protected by products containing either NSA certified or National Institute of Standards and Technology (NIST) validated cryptographic modules.

4.8. All systems within the GNIE shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (k)).

4.9. All system connections to non-DoD information systems, to include foreign nation systems, shall be accomplished in accordance with established connection approval processes for the network (e.g. SIPRNET procedures, NIPRNET procedures, etc.)

4.10. Access to GNIE systems will be in accordance with DoD Regulation 5200.2R (reference (l)). *(This paragraph will be expanded)*

4.11. Interconnection of systems operating at different classification levels shall be accomplished by processes (e.g., Secret and Below Interoperability (SABI) reference (m)) that have been approved by the DoD Chief Information Officer (CIO).

4.12. DoD information systems that allow open, uncontrolled access to information made available by the Department, such as information intended for dissemination to the general public (e.g. publicly accessible web servers), or systems that allow unregulated access to and from the Internet shall be isolated. The isolation may be physical, or may be implemented by technical means such as an approved boundary protection product in accordance with the DoD policy for web site administration (reference (n)).

4.13. All systems within the GNIE are subject to monitoring in accordance with DoD Directive 4640.6 (reference (o)), to include active penetrations and other forms of testing used to complement monitoring activities, in accordance with applicable laws and regulations.

4.14. Use of public key certificates in GNIE systems shall be consistent with DoD certificate policies promulgated by the ASD(C3I) . *(Will be modified and the appropriate reference added)*

4.15. All DoD personnel shall be trained and appropriately certified to perform the tasks associated with their designated responsibilities for safeguarding and operating GNIE systems in accordance with joint USD (P&R) and ASD(C3I) guidance (reference (p)).

4.16. Commercial-off-the-shelf (COTS) products shall be used in all systems consistent with the requirements of this policy memorandum.

4.17. Public domain products shall not be used unless appropriately assessed for information assurance impacts.

4.18. All hardware, firmware, and software security related components ( excluding cryptographic modules) acquired to protect systems within the GNIE shall be evaluated and validated prior to installation and use, using criteria and processes established by NSA. The assemblage (i.e., installation, integration and use) of these components into an IA configuration will be subject to systems security analysis prior to system accreditation.

4.19. All systems shall be managed and operated to achieve the appropriate level of protection in accordance with Part II of this memorandum.

4.20. Only NSA evaluated and validated IA products, techniques and services shall be used to protect classified information.

4.21. DoD Components shall acquire COMSEC products and services to protect classified systems through the NSA as the centralized COMSEC acquisition authority or, if the products or services are unavailable through centralized procurement, from CIO approved commercial sources.

4.22. Sensitive information shall be protected by use of National Institute of Standards and Technology (NIST) validated products and techniques.

5. RESPONSIBILITIES:

5.1. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)), in his capacity as the DoD Chief Information Officer (CIO), shall:

5.1.1. Monitor and provide oversight for all DoD IA activities.

5.1.2. Develop and promulgate other IA guidance regarding the GNIE consistent with this memorandum.

5.1.3. Ensure that all systems are assigned to a mission category not later than one year from the date of this document.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection (reference (q)).

5.1.4. Ensure proper protection of Intelligence Comity (IC) data on DoD networks.

5.2. The Heads of DoD Components shall:

5.2.1. Ensure compliance with this policy memorandum.

5.2.2. Develop and implement an IA program in accordance with the requirements of this policy memorandum focusing on protection of Component-specific portions of the GNIE (i.e., sustaining base, tactical, C4I interfaces to weapon systems, etc.)

5.2.3. Plan, budget and execute adequate resources in support of IA for the GNIE.

5.2.4. Ensure that Designated Approving Authorities (DAAs) accredit each information system under their jurisdiction.

5.2.5. Develop Memorandums of Agreement (MOA), as appropriate, for connection of

information systems managed by multiple DAAs.

5.2.6. Assign mission categories to Component-specific systems not later than (*date TBD*).

5.2.7. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all system technologies and supporting infrastructures.

5.2.8. Ensure that IA awareness, training, education, and professionalization are provided to all personnel commensurate with their respective responsibilities for using, operating, administering, and maintaining systems within the GNIE in accordance with reference (p).

5.2.9. Comply with established connection approval processes for all information systems connections.

5.2.10. Share techniques, technologies, and R&D relating to IA with other DoD components.

5.2.11. Provide for an IA monitoring and testing capability in accordance with reference (o) and applicable laws and regulations.

5.2.12. Provide for a vulnerability and incident response and reporting capability.

5.2.13. Coordinate with and report all systems security incidents to the Joint Task Force – Computer Network Defense (JTF-CND) in accordance with CJCS instructions.

5.2.14. Take action in response to Information Operation Conditions (INFOCONs) as directed by the CJCS.

5.2.15. Comply with DoD COMSEC instructions and regulations.

5.2.16. Ensure that requirements to protect classified and sensitive unclassified information are provided to their contractors and agents.

5.2.17. Ensure that all COTS products acquired for security functions have been evaluated under criteria established by NSA.

5.3. The Chairman, Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.2., shall:

5.3.1. Ensure that Unified Combatant Commanders incorporate appropriate IA elements in the generation of requirements for systems support to Joint and Combined operations.

5.3.2. Review and approve foreign nation access to DoD-wide elements of the GNIE (e.g., DISN).

5.3.2. Recommend changes in the DoD Information Operations Condition INFOCON to the Secretary of Defense

5.4. The Commander, JTF-CND shall:

5.4.1 Coordinate and direct DoD-wide computer network defense operations to include:

5.4.1.1. Actions necessary for a synchronized defense of DoD computer systems and networks e.g., network patches, firewall rules).

5.4.1.2. Actions necessary to stop a computer network attack (CNA), limit damage from a CNA, and restore effective computer network service following a CNA.

5.4.2 When directed by the Secretary of Defense, issue INFOCONs to alert DoD Components of DoD-wide cyber situations that threaten the GNIE and require increased awareness and specific defensive postures

5.5. The Director, National Security Agency (NSA), in addition to responsibilities specified in paragraph 5.2., shall:

5.5.1. Implement an IA intelligence capability responsive to requirements for DoD, less DIA responsibilities.

5.5.2. Provide IA services to DoD Components as required to assess the threat to, and vulnerability of, IA technologies.

5.5.3. Serve as the DoD focal point for INFOSEC R&D in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.5.4. Lead the development of an IA technical framework for defense-in-depth strategy and provide engineering support and other technical assistance for its implementation within DoD..

5.5.5. Establish and manage a program for the evaluation and validation testing of commercially developed IA products in categories directed by the DoD CIO.

5.5.6. Coordinate activities of the National Security Incident Response Center (NSIRC) (reference (s)) with other DoD Components to integrate NSIRC efforts into protection of the enterprise.

5.6. The Director, Defense Intelligence Agency (DIA), in addition to the responsibilities specified in paragraph 5.2. shall:

5.6.1. Provide finished intelligence on IA affecting the GNIE to DoD Components.

5.6.2. Develop, implement, and oversee an IA program for layered protection of the DoDIIS element of the GNIE.

5.6.3. Manage the approval process for connection of intelligence systems to the GNIE

5.7. The Director, Defense Information Systems Agency (DISA), in addition to the responsibilities specified in paragraph 5.2. shall:

5.7.1. In coordination with NSA, develop, implement and oversee a single IA strategy for layered protection of the DoD-wide elements of the GNIE.

5.7.2. Manage connection approval processes for the DoD –wide elements of the GNIE (e.g., Defense Information Systems Network (DISN), SIPRNET).

5.7.3. Operate and maintain, in coordination with the other DoD Components, a GNIE information system monitoring and incident response center.

5.7.4. Coordinate with and support the JTF-CND.

5.7.5. In coordination with the Joint Staff, NSA, and DIA as required, maintain security accreditation of the DoD-wide elements of the GNIE.

5.8. Each Designated Approving Authority (DAA) shall:

5.8.1. Be responsible for the security of all systems under their jurisdiction.

5.8.2. Review and approve security safeguards and issue accreditation statements for each system under their jurisdiction, based on the acceptability of the safeguards and compliance with reference (k).

5.8.3. Ensure that all required safeguards, as specified in accreditation documentation, are implemented and maintained.

5.8.4. Identify security deficiencies and initiate appropriate action to achieve an acceptable security level as required.

5.8.5. Ensure that an Information Systems Security Manager (ISSM), Information Systems

Security Officers (ISSOs) and Systems Administrators (SAs) are designated for each system under their jurisdiction, and that they receive the level of training necessary and appropriate certification to perform the tasks associated with their assigned responsibilities.

5.8.6. Verify that data ownership is established for each system under their jurisdiction and that the system has been assigned to a mission category.

5.9. Each Information Systems Security Manager (ISSM) shall:

5.9.1. Serve as the focal point for policy and guidance on IA matters within their activity.

5.9.2. Provide policy and program guidance to subordinate activities.

5.10. Each Information Systems Security Officer (ISSO) shall:

5.10.1. Ensure that systems for which they have cognizance are operated, used, maintained, and disposed of in accordance with the system accreditation package security policies and practices.

5.10.2. Have the authority to enforce IA policies and safeguards on all personnel having access to the system for which the ISSO has cognizance.

5.10.3. Ensure that users have the required security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with required security practices prior to being granted access to the system.

5.10.4. Ensure that audit trails are reviewed periodically.

5.10.5. Report all security incidents.

5.10.6. Report on the IA posture of the information system, as required by the DAA.

5.11. Each System Administrator (SA) shall:

5.11.1. Work closely with the ISSO to ensure the system is used properly.

5.11.2. Assist the ISSO in maintaining configuration control of the system.

5.11.3. Advise the ISSO of security anomalies or integrity loopholes.

5.11.4. Administer, when applicable, user identification or authentication mechanism(s) of the system.



5.11.5. Perform system backups, software upgrades and system recovery, including the secure storage and distribution of backups and upgrades.

6. EFFECTIVE DATE: This policy is effective immediately.

## Part II

## Implementation Guidance

1. OVERVIEW

1.1. This section and associated references provide additional guidance on the selection of appropriate security technical countermeasures (e.g. TEMPEST, trusted operating systems and applications, personal tokens, enclave boarder and network protection devices, security infrastructure devices, etc.) and non-technical countermeasures (e.g. acquisition; assessment; certification; accreditation policy and procedures, etc.) related to Information Assurance Security Requirements. Additional, more detailed guidance on information assurance products and system design is provided in the Information Assurance Technical Framework (previously know as the Network Security Framework) which may be found at <http://www.nsff.org> on the World Wide Web.

1.2 All Information Technology (IT) system designs and implementations shall use the guidance and incorporate the required analysis and mechanisms as detailed in this document and all referenced documents. Detailed requirements for specific IT implementations shall be dependent upon an in-depth system security analysis and evaluation which must take into consideration the functional domain information owner-assigned mission category (also referred to as “information value”), threat which is applicable to the specific user’s mission, and assigns an appropriate level of information assurance required (also referred to a ‘level of required robustness’).”

2. MISSION CATEGORIES

2.1 All DoD systems within the GNIE shall be assigned to a mission category by the DoD functional domain owner, in consultation with the information owner.

2.1.1. The *DoD functional domain owner* is defined as the responsible DoD component senior official for each of the missions areas that are necessary to the achievement of DoD goals and objectives, particularly the warfighter’s combat mission (e.g. logistics, transportation, medical, intelligence, personnel, financial).

2.1.2. The *functional domain information owner* (also referred to an information owner) refers to organizational personnel who create and are responsible for managing specific information related to their assigned DoD functional mission area.

2.2. The DoD *mission categories* are established based on the type of the information handled (i.e., entered, processed, stored, displayed, or transmitted) by the system relative to the achievement of DoD goals and objectives and are defined as follows:

2.1.1. Mission Critical: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). Typically, critical mission category information is threatened by extremely sophisticated adversaries willing to expend abundant resources, and encounter up-to extreme risk (e.g. well-funded national laboratory, nation-states, international corporations, well-funded terrorists, etc.) Typically, violation of critical mission category information, and associated protection policies, would adversely affect and/or cause exceptionally grave damage to the security, safety, financial posture, and/or infrastructure of the DoD mission.

2.2.2. Mission Support: Systems handling information that is important to the support of deployed and contingency forces; must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information). Typically, support mission category information is threatened by sophisticated adversaries willing to expend moderate resources, and encounter significant risk (e.g. organized crime, sophisticated hackers, international corporations, international terrorists, etc.). Typically, violation of support mission category information, and associated protection policies, would adversely affect and/or cause serious damage to the security, safety, financial posture, and/or infrastructure of the DoD mission.

2.2.3. Administrative: Systems handling information which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (likely to be sensitive or unclassified information). Every effort to ensure that the accuracy and availability of administrative mission category information should typically be made, however it is recognized that this information may be recreated should the need arise. Typically, administrative mission category information is threatened by inadvertent/accidental events or passive/casual adversaries, willing to expend minimal resources and encounter moderate risk (e.g. poorly trained users, unsophisticated hackers). Typically, violation of administrative mission category, and associated information protection policies would adversely affect and/or cause minimal damage to the security, safety, financial posture, and/or infrastructure of the DoD mission.

### 3. LEVELS OF PROTECTION

3.1. Each DoD information system and network must be managed and operated in accordance with the requirements of an appropriate assurance level. Determination of appropriate levels of information assurance is not a trivial exercise and is dependent on an in-depth system security analysis and evaluation which must take into consideration the functional domain information owner-assigned mission category (also referred to as “information value”), threat which is applicable to the specific user’s mission and actual analysis/testing of selected components; interfaces and implementation details.

3.2 IA is a critical component of DoD operational readiness and mission effectiveness, and as such, the level of protection required to support mission accomplishment shall be evaluated for each network and information system. The extent to which IA protective measures, techniques and procedures must be applied shall be assigned a level of protection based on mission criticality, risk, threat, vulnerability, system interconnectivity considerations, and specific assurance needs, in conjunction with the appropriate Designated Approving Authority (DAA). Assigned levels of assurance shall fall into one of three categories:

3.2.1. High: Information systems that require the most stringent protection and rigorous security countermeasures. This level of IA is mandated for critical category information; actual selection of security technical and non-technical mechanisms and system design must result from a thorough system security analysis and extensive evaluation.

3.2.2. Medium: Information systems that require increased layering of additional safeguards above the DoD standard minimum-security countermeasures. Though this level of protection is typically appropriate for support mission category information, actual selection of security technical and non-technical mechanisms and system design must result from a through system security analysis and evaluation.

3.2.3. Basic: Information systems that require implementation of the DoD standard minimum-security countermeasures equivalent to good commercial practice. It is resistant to the unsophisticated threat and is used to protect low value data. Though this level of protection is typically appropriate for administrative mission category information, actual selection of security technical and non-technical mechanisms and system design should result from at least a cursory system security analysis and evaluation.

3.3. To assist in a system security analysis and evaluation, refer to chapter 4.4 of the Information Assurance Technical Framework (previously known as the Network Security Framework) at <http://www.nsff.org> on the World Wide Web.

3.4. The following information is provided as a tool to be used to assist in a system security analysis and evaluation to determine the level of protection needed for the components and system being evaluated.

Information values:

V1: Violation of the information protection policy would cause *some damage* to the security, safety, financial posture, stature or integrity, and/or infrastructure of the organization. Examples are; privacy act data, medical records, unclassified mission critical data, government sensitive but unclassified data, company proprietary data, small financial transactions, and minor operational disruptions.

V2: Violation of the information protection policy would cause *serious damage* to the security, safety, financial posture, stature or integrity, and/or infrastructure of the

organization. Examples are government confidential releasable, secret releasable, confidential, secret, secret compartmented data, company trade secrets, large financial transactions, and short-term operational operations .

V3: Violation of the information protection policy would cause *exceptionally grave damage* to the security, safety, financial posture, stature or integrity, and/or infrastructure of the organization. Examples are government top secret releasable, top secret, top secret compartmented data, highly important company trade secrets, very large financial transactions, and long-term operational disruptions.

Threat levels:

T1: No known adversary or an adversary without determination. Concerned mostly with inadvertent errors of disclosure or modification of information or denial of service (e.g. threat to an average home computer connected to the Internet).

T2: Adversary with minimal resources, somewhat sophisticated, willing to take moderate risks (e.g. single hacker with determination, small company).

T3: Adversary with adequate or more resources, willing to take moderate or more risk or whatever risk is necessary to be successful, sophisticated or able to purchase sophisticated help (e.g. organized hackers, organized crime, large corporations, terrorists, nation states, national labs).

	T1	T2	T3
V1	SML 1 EAL 1 Basic Medium	SML 2 EAL 3 Medium Medium	SML 2 EAL 3 Medium High
V2	SML 2 EAL 3 High	SML 2 EAL 3 High	SML 3 EAL 6 High
V3	SML 2 EAL 3	SML 3 EAL 6	SML 3 EAL 6

Level of protection table

SML 1 EAL 1 = basic level of protection;  
SML 2 EAL 3 = medium level of protection;  
SML 3 EAL 6 = high level of protection.

SML = Strength of Mechanism Level

EAL = Evaluated Assurance Level (see the Common Criteria for a detailed description)

3.4. It can be seen from the above chart how threat plays a role in determining the level of protection. One can not directly relate value of information with strength of mechanism since if the threat is low a weaker level of protection may be appropriate. Of course the reverse is also true, if the threat is high, lower value information may require a higher level of protection. An example of protecting high value information in a low threat environment would be data on the SIPRNET. Data needs access control protection for need to know purposes, however, since it on the SIPRNET a lower level of protection may be acceptable.

#### 4. INFORMATION ASSURANCE (IA) CONSIDERATIONS

##### 4.1 General IA Considerations

4.1.1 Layered Defense Strategy: Required levels of IA shall be achieved via a layered defense strategy (also referred to as “defense-in-depth”), incorporating appropriate safeguards from the spectrum of the INFOSEC disciplines. Both technical and non-technical security measures can assist in mitigating risk, and as such, shall be integrated with the objective of protecting DoD information technology resources. Appropriate countermeasures provided by these disciplines shall be applied to each DoD information system and site security policy, through a system security analysis assessment of the capability and probability of a threat, and the risk resulting from unauthorized disclosure, destruction, alteration, or non-availability of information or resources supporting the DoD mission. Information entered, processed, stored or transmitted shall not exceed the approved classification or sensitivity level for the system or network. Use of the IA disciplines shall be carefully managed, regularly reviewed and continuously monitored throughout the lifecycle of information technology resources. Both technical and non-technical mechanisms supporting a layered defense strategy are itemized in the subsequent sections. Additional details related to the Layered Defense Strategy can be obtained on the World Wide Web at location <http://www.nsff.org>.

4.1.2. System Security Standards: Failure to implement sound security procedures during system design may compromise the effectiveness of technical security countermeasures (e.g. packet filtering, routers, firewalls, etc.). Though it may appear that appropriate security features have been incorporated at the individual system level, unanticipated vulnerabilities may surface when inter-operating with other systems over shared communication links. DAAs must consider the inherent risk of operating less secure systems inside a secure enclave. To the extent possible, legacy systems shall employ system security standards that support appropriate security protocols within a secure enclave. Modifications to legacy systems should prioritize incorporation of common security procedures and products to improve their overall security postures. Those legacy systems with insecure security

implementations should be placed outside the secure enclave or in a separate “safe” zone if they pose significant security risks to other information resources protected within the enclave. Additional information related to the system security standards can be obtained from the NIST Federal Information Processing Standards on Computer Security World Wide Web Site at location <http://csrc.nist.gov/fips/>.

4.1.3 Five Properties of Information Assurance: Information technology resources must be properly managed and protected as required by law, regulation or treaty. Facilitating the management and protection of resources requires the appropriate implementation of security measures to ensure adequate system protection is applied for safeguarding the IA properties of:

4.1.3.1. **Confidentiality**, which supports the protection of both sensitive and classified information from unauthorized disclosure.

4.1.3.2 **Integrity**, which supports protection of information and information systems from unauthorized modification or destruction.

4.1.3.3. **Availability**, which supports timely, reliable access to information and information systems for authorized users, and precludes denial of service/access.

4.1.3.4. **Authenticity**, which supports verifying an individual's identity and authorization to access specific categories of information and information systems.

4.1.3.4. **Non-repudiation**, which provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

Information Assurance is a composite of the five properties described above. Protection shall be achieved through the cost-effective, risk-balanced use of the security disciplines, based on the appropriate level of IA required. These properties may be integrated into security services.

4.1.4. Information System Security Policy (ISSP): An Information System Security Policy shall be developed and maintained for every DoD organization employing information technology resources and for each information system used within the DoD. The ISSP shall identify the security requirements, objectives and policies implemented to safeguard the site or system in a prescribed operational configuration. This policy document will become part of the SSAA required by the DISTCAP (reference (j)).

4.1.5 Use of Appropriate Generic Security Architectures: The following is a brief description of seven generic security architectures that address different aspects of typical mission functionality. This list is not necessarily all-inclusive, but is intended to serve as a tool to assist in describing various GNIE functional configurations that should be considered when performing a system security analysis. (For additional details on the following generic security architectures, please refer to

Section 5 of the Information Assurance technical Framework (previously know as the Network Security Framework) at <http://www.nsff.org> on the World Wide Web.)

4.1.5.1. System High Interconnections and Virtual Private Networks providing secure connectivity between systems (LANs, Hosts, Client Workstations, ? ) operating at the same sensitivity levels via backbone networks while protecting against the outsider threat.

4.1.5.2. Protection for Network Access protecting information and resources of a network from intrusion resulting in the compromise of Confidentiality, Integrity, or Availability when connecting to potentially hostile networks for the purpose of obtaining information and services from those networks.

4.1.5.2 Remote Access providing traveling or work-at-home users with secure access to their local LANs, enclaves, or enterprise computing environments.

4.1.5.3. Multi-Level Security (MLS), containing two subcategories: High-to-Low providing the ability to exchange low side data to and from High side LANs and MLS Workstations, Servers, and Networking Components

4.1.5.4. Security for System Applications providing identification and authentication (I&A), access control, confidentiality, data integrity, and non-repudiation services for the variety of legacy and emerging applications within system high environments.

4.1.5.5. Availability of Backbone Networks ensuring that the various government and commercial backbone networks (e.g., voice, data, cellular, satellite) provide the requisite degree of operational availability in terms of their ability to support the reliable transport of user data. This category focuses on a principal aspect of Information Assurance, protection against Denial-of-Service attacks and the ability to recover from such attacks.

4.1.5.6. Security Management Infrastructure (SMI) including the SMI technologies that provides security management services to the security products that provide security services for the above categories.

## 4.2. Non-Technical Countermeasures

4.2.1. Connection Approval: Information system and network connections within the GNIE shall be in accordance with the established connection approval processes for the network (e.g. SIPRNET procedures, NIPRNET procedures) to ensure the appropriate level of IA is maintained. Connection approval processes shall also be applied to GNIE systems and networks connected to external, non-DoD, coalition, and combined systems and networks.

4.2.1.1 Connection of Systems at Different Classification Levels: Interconnection of systems operating at different classification levels shall be accomplished by processes (e.g., Secret and Below Interoperability (SABI) reference (I)) that have been approved by the DoD



Chief Information Officer (CIO).

4.2.1.2. Systems with Uncontrolled Access: GNIE information systems that allow open, uncontrolled access, such as information intended for dissemination to the general public (e.g. publicly accessible web servers), or systems that allow unregulated access to and from the Internet shall be isolated. The isolation may be physical, or may be implemented by technical means such as an approved boundary protection product in accordance with the DoD policy for web site administration (reference (m)).

4.2.2. Personnel Security Training and Certification: All DoD personnel shall be trained and appropriately certified to perform the tasks associated with their designated responsibilities for safeguarding and operating GNIE systems in accordance with joint USD (P&R) and ASD (C3I) guidance (reference (p)). For additional information see the DOD Directive 5200.2, Department of Defense Personnel Security Program (DoD PSP), at the World Wide Web site, <http://web7.whs.osd.mil/text/d52002p.txt>.

4.2.3. Physical Security: Physical Security is the action taken to protect DoD information technology resources (e.g. installations, personnel, equipment, electronic media, documents, etc.) from damage, loss, theft, or unauthorized physical access. For additional information see the DOD Directive 5200.8, Security of DoD Installations and Resources, at the World Wide Web site, <http://web7.whs.osd.mil/text/d52008p.txt>

4.2.4. Procedural Security: Procedural Security, including operational security (OPSEC) measures, can provide an alternative to technical security means when risk analysis indicates the use of procedures does not increase the overall risk to a system or network. Procedural Security provides the necessary actions, controls, processes, and plans to ensure contiguous operation of a system or network within an accredited security posture, and is site and task dependent. Site security procedures shall be developed to supplement the security features of the hardware, software and firmware of information technology resources, to include such standardized processes as user access control, media labeling and classified material handling. For additional information, see the DOD Directive 5205.2, DoD Operations Security Program, at the World Wide Web site, <http://web7.whs.osd.mil/text/d52052p.txt>.

#### 4.2.5. Product/Module Certification

4.2.5.1. Only National Security Agency (NSA) certified cryptographic modules shall be employed in products used to encrypt classified information or sensitive information delineated by Title 10, United States Code, Section 2315 (reference (h)).

4.2.5.2. Sensitive information subject to Public Law 100-235 (reference (i)) shall be protected by products containing either NSA certified or National Institute of Standards and Technology (NIST) validated cryptographic modules.

4.2.6. Vulnerability Assessments: Assistance is available to assess and improve the IA posture, by identifying vulnerabilities in an operational environment and validating a particular site's overall security posture and degree of system integration.

4.2.6.1. On-line Surveys: When requested, \_\_\_\_ will conduct on-line surveys of NIPRNET, SIPRNET and Joint Warrior Intelligence Community System (JWICS) networks to help DoD commands identify vulnerabilities on these systems.

4.2.6.2 On-site Assessments: To improve their security posture, commands may request more detailed on-site assistance.

4.2.6.3. Red Team Operations: Red Team operations may be employed to validate existing IA protections and to exercise standard operating procedures and tactics to evaluate vulnerabilities.

#### 4.3 Technical Countermeasures

4.3.1 Emanations Security (TEMPEST): Electronic communications can produce unintentional, intelligence-bearing emanations that, if intercepted and analyzed, may disclose information transmitted, received, handled, or otherwise processed. TEMPEST countermeasures shall be used in proportion to the threat of exploitation and the associated potential damage to national security, as recommended by a DoD Certified TEMPEST Technical Authority (CTTA), in accordance with reference (f), which provides specific objectives for reducing or eliminating unintentional emanations.

4.3.2. Remote Access and Remote Management: Remote control or use of remote management software protocols shall, in general, be discontinued. Uncontrolled and non-secure remote access to GNIE information systems and networks potentially bypass other system security measures. Sites with either dial-up or wide area networked remote access capability may only by exception and explicit approval incorporate access controls and authentication procedures (i.e. one-time passwords or X.509 Certificates, etc.), selected to be commensurate with the classification or sensitivity level of the data and systems involved. Authentication procedures must verify the identity of the user, as well as control access to specific systems and data. An approved GNIE, DoD warning banner shall be displayed at the network and system level upon establishment of each remote access session.









4.3.3. Firewalls: Firewalls are a class of security products that control the flow of traffic between networks operating under disparate Information System Security Policies (ISSPs.) Firewalls typically incorporate security techniques such as packet filtering, application proxies, access control filters, and state inspection. Firewall protection techniques may be achieved via a specifically designed product, or through inherent capabilities within existing resources. Mere presence of a firewall does not ensure adequate protection. The firewall must be correctly configured to match the technical architecture of the operating environment and enforce the appropriate system security policy/procedures

protecting information and resources from unauthorized internal or external compromise.

4.3.4. Mobile Computing: Mobile-computing poses issues of physical security, as well as remote access. Appropriate physical security measures shall be employed to protect the mobile hardware, software and data contained therein, or data accessible via the mobile hardware, commensurate with the classification or sensitivity level of the data and systems involved. Specific safeguards, such as approved encryption mechanisms, should be employed to protect information in the event the mobile hardware falls into unauthorized control.

4.3.5. Information Systems Infrastructure: Networked information systems may incur additional risks because of the exposure of their data and resources to a larger community of users. GNIE systems must utilize standard approved, enterprise-wide security infrastructure

4.3.6. Virus and Malicious Code Protection: The threat of attack from computer virus or other malicious code, both deliberate and inadvertent, is significant. Successful virus prevention incorporates technical, policy and procedural elements. All GNIE information systems and networks shall use approved anti-virus software to intercept viruses before they can establish themselves. DoD functional domain owners shall develop and implement local policy and procedures to support effective employment of anti-virus software and should address:

-  Stand Alone and Macro Viruses
-  Java and Active-X Scripts
-  Cookies
-  Web Casting
-  Floppy Disks
-  Notebook and Privately Owned/Home Computers
-  Email Attachments
-  Downloaded and Remotely Transferred Files

4.3.6.1 As the nature of the threat from virus software constantly changes, sites shall ensure that anti-virus software profiles are updated frequently and on a routine basis. DoD licensed anti-virus software is available free to all DoD activities. This software is also authorized for, and should be installed on, personal computers, privately owned by DoD personnel, used for official business

4.3.7 Certificate Management: Properly employed public key based security mechanisms provide a good means to protect GNIE information systems from unauthorized access and to provide access control to system resources. Only approved workstations shall be used for certificate establishment and management services. Addition information related to Certificate Policy and Public Key Infrastructure can be obtained on the World Wide Web at location <http://www.nsff.org>.

## 5. IMPLEMENTATION:

5.1. Resources: Resources sufficient to ensure compliance with this policy memorandum shall

be planned, budgeted, allocated and executed.

5.2. COTS Products: Consistent with security policies and good security practices, commercial-off-the-shelf (COTS) products will be used where possible in all information assurance applications.

5.3. Product Validation: All hardware and software security related components acquired to protect systems within the GNIE shall be evaluated and validated prior to installation and use, using criteria established by NSA.

5.4. Certification and Accreditation: All DoD information systems and networks shall be certified and accredited in accordance with DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)” (reference (j)), see World Wide Web Site <http://mattche.iie.disa.mil/ditscap/index.html>.

## 6. OPERATIONS

6.1. Standard Operating Procedures: Consistent, clearly documented operating procedures for both system configuration and operational use are key to ensuring information assurance. Procedures should define deployment of the system, system configuration, day to day operations for both the system administrator and user, as well as how to respond to real or perceived attempts to violate system security. All DoD information systems and networks shall include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment.

6.2. Access: Access to GNIE systems will be in accordance with DoD Regulation 5200.2R (reference (k)).

6.3. Use of PKI Certificates: Use of public key certificates in GNIE systems shall be consistent with DoD certificate policies promulgated by the ASD(C3I). Additional information related to Certificate Policy and Public Key Infrastructure can be obtained on the World Wide Web at location <http://www.nsff.org>.

6.4. Contingency Planning: Given the dependencies of today’s operations on information technology resources, all DoD units must be prepared for worst case contingencies in the event of the non-availability of information systems and resources or denial of service conditions. Requirements for system redundancy and data backup should be incorporated in a system and network design, based on the level of IA that is required. Contingency plans shall be developed and tested to prepare for emergency response, backup operations, and post-disaster recovery. At a minimum, contingency planning shall address reconstitution for the loss of processing, storage or transmitting of information.

6.5. Monitoring: All systems within the GNIE are subject to monitoring in accordance with DoD Directive 4640.6 (reference (n)), to include active penetrations and other forms of testing used to complement monitoring activities, in accordance with applicable laws and regulations. All individuals attempting access to DoD information systems shall be provided sufficient notice that use of official DoD information systems or networks constitutes consent to monitoring. Adequate warning shall be provided by clearly displaying the legally approved DoD warning banner. At a minimum, the DoD warning banner

shall be displayed to the user upon initial entry/login to system, network, local, and remote resources. Acceptance of the banner warning screen shall constitute consent to monitoring.

6.6. Security Incident Procedures: In addition to protective measures designed into information systems and architectures, sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of DoD operations.

6.6.1. Network Management Tools: Network management tools that detect, isolate, and react to intrusions, disruption of services, or incidents that threaten the security of DoD information technology resources shall be used.

6.6.2. COMSEC Material Incident Response: Incidents involving the compromise or the suspected compromise of COMSEC material or incidents that warrant further investigation shall be reported in accordance with procedures established in the DoD IA Publications.

6.6.3. Computer Incident Response: In accordance with reference (\_\_\_), the \_\_\_, located at \_\_\_, serves as the DoD primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten DoD information systems and networks. The \_\_\_ will collaborate and coordinate DoD efforts with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

6.6.4 Incident Reporting: All DoD organizations shall promptly report incidents that threaten DoD information and resources to \_\_\_ in accordance reference (\_\_\_). This reporting requirement does not preclude operational commanders from establishing parallel reporting requirements within their assigned area of operations or does it alleviate or replace any additional reporting requirements established by the chain of command. The following types of incidents shall be reported:

~~///~~ Computer Intrusions: Unauthorized access to data or to an automated information system.

~~///~~ Attempted Intrusions: Unauthorized, unsuccessful attempts to access data or an automated information system.

~~///~~ Denial of Service Attacks: Actions which prevent any part of an automated information system from functioning in accordance with its intended purpose, to include any action which causes the unauthorized destruction, modification, or delay of service.

~~///~~ Malicious Logic: Hardware, software, or firmware that is intentionally included in an information system for an unauthorized purpose, such as a virus or Trojan horse.

~~///~~ Probes: Any attempt to gather information about an automated information system or its users online.

## 7. SYSTEM MANAGEMENT

7.1. IA Management: Information assurance shall be managed to ensure that the principles contained in this policy memorandum are included in the decision-making processes throughout the entire life cycle of all systems within the GNIE in accordance with DoD Regulation 5200.1R (reference (g)).

7.2. Configuration Management: Configuration management identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational lifecycle. Proper configuration management can substantially reduce and sometimes eliminate the need for costly complete re-accreditation. Appropriate levels of configuration management shall be established to maintain the accredited security posture. Each change or modification to an information system or site configuration shall assess the security impact of such a change against the security requirements and the accreditation conditions issued by the DAA.

7.3. Data Management: The increasing reliance on distributed, interconnected information systems negates many of the data protection mechanisms built in to traditional "system high" networks and requires additional safeguards to protect DoD information from both unauthorized users and from authorized users without a need to know. Data processed, transmitted and stored on DoD information systems shall be protected to the appropriate level of classification or sensitivity and required level of IA. All DoD Components will implement mechanisms for the electronic labeling of data processed, transmitted, stored, or displayed on DoD information systems.

7.3.1. Data Marking: Electronic data and files shall be marked to reflect the appropriate classification or sensitivity. At a minimum, all electronic information in the form of documents, images, or other human-viewable format, regardless of location, shall include plain-text markings indicating classification or sensitivity, as would be required if they were hardcopy products.

7.3.2. Data Release: Data, both physical (e.g., hard copy) and electronic (e.g., floppy disks, web pages), shall be released in accordance with established DoD data release procedures. Sharing of information with allied and coalition personnel shall be in accordance with the provisions of reference (h).

7.3.3. Data Access: Appropriate procedures for establishing and disestablishing access and authentication shall be based on need to know and the classification or sensitivity level of the information. Authentication and access control may be enforced by the operating system or through encryption techniques.

7.4. Password Management: Passwords are one of the simplest, most effective security measures, but are often the first target of intruders. Passwords shall be managed in accordance with the guidelines of reference (r), tailored to the appropriate level of protection required.

7.4.1 Password Formats: Passwords shall be a minimum of eight characters in length, consist of a mixture of alphabetic and numeric characters or numerals, and avoid the use of names and dictionary words. System Administrators should use tools from the IA Help Desk to evaluate the vulnerability of passwords under their control. Legacy systems constrained by system design may be exempt from the eight-character password length requirement, with the approval of the DAA.

7.4.2. Default Passwords: Accounts shall not be issued with default passwords (i.e., "password"). Default passwords at the system or network administrator level shall be changed to a site unique password upon system installation, and verified prior to final system accreditation.

7.4.3. Password File Protection: Password files shall be appropriately protected from access by intruders.

7.4.4. Password Updates: Passwords shall be changed quarterly, at a minimum, for systems with automated password administration capability. All other systems shall change passwords annually at a minimum. If supported, automated password administration features should be employed to ensure choice of sophisticated passwords and preclude reuse of previously employed passwords.

7.5 Account Management: System administrators shall monitor user account inactivity and establish procedures for investigating, deactivating and eliminating accounts that do not show activity over time. For example, deactivate accounts with no activity for over 30 days, and investigate and eliminate accounts with no activity for over 90 days. Applicability and associated privileges of all default accounts shall be validated and deactivated, as appropriate, prior to system accreditation.

7.6. Use of Personal Hardware and Software: Official DoD business shall normally be conducted using government owned resources. Local policies and procedures controlling the use of personal hardware and software shall be established to include the use of anti-virus software. Processing of classified information using personally owned or leased hardware and software is specifically prohibited. Software that is personally procured or developed, or obtained as "public domain" or "shareware," shall not be installed on government owned systems without Information System Security Manager (ISSM) and System Administrator evaluation for compatibility, correct operation and absence of viruses.

7.7. Risk Management: Protection of information technology resources requires a balanced, risk-based approach, managing the requirements of the system or resources against a cost-effective application of technical and non-technical security disciplines and technologies to mitigate the risks. Identification, measurement, control, and minimization of security risks to a level commensurate with the value of the assets protected shall be considered. Formal risk assessments for DoD information systems and resources may be tailored, at the direction of the DAA, to the criticality and level of the IA threat.

## **8.. ADVANCED GUIDANCE FOR IMPLEMENTERS**

8.1. Level of Protection Tables: The following tables are provided as guidance for system security engineers. They can be use to help provide information for analysis of requirements and solutions. There is no one size fits all in the DoD community. However, good system security engineering is required to ensure good defense in depth solutions.

8.1.1. The level of protection required for a security service (i.e., confidentiality, integrity and availability) is based on a combination of factors, as discussed in Paragraph 3 above.

8.1.1.1. The principal factors are the mission category of the information (integrity and availability services) and the classification or sensitivity of the information (confidentiality service).

8.1.1.2. Additional factors that affect the level of protection are interconnectivity considerations and the operating environment (see definition in Part IV).

8.2. As discussed in Paragraph 8.1c, the following chart depicts the **minimum** level of protection for each security service:

Factor		Security Service & Minimum Protection Levels	
Mission Category		Integrity (includes authentication and non-repudiation)	Availability
Mission Critical		High	High
Mission Support		Medium	Medium
Administrative		Basic	Basic
Information Sensitivity		Confidentiality	
Classified		High	
Sensitive (including FOUO, Privacy Act, Financial, Medical, Proprietary, Logistics)		Medium	
Format Sensitive (Aggregated Data)		Medium	
Information that is Both Unclassified & not sensitive		Basic	
Interconnectivity Considerations		Will impact the level of protection required for selected security functions (e.g., direct connection of a system requiring basic confidentiality to one requiring medium confidentiality will require the connected system to have medium confidentiality despite the fact that none of the information it handles is sensitive.	
Operating Environment		May affect the method of implementing required security functions within the selected level of protection	



## 8.2 Determining the required Level of Protection:

8.2.1. “Basic” is the minimum acceptable level of protection for DoD GNIE systems and must be applied to all security services implemented.

8.2.2. The level of protection need not be the same for each security service; e.g., systems processing mission critical information will always require a high level of protection for integrity and availability, but may require only the basic level of protection for confidentiality.

8.3. Once the level of protection for the three security services is determined, individual security functions can be selected and implemented. The following matrix is provided to assist in selecting security functions and capabilities to support the various levels of protection. Individual security functions may support multiple security services (e.g., access control can support the security services of confidentiality, integrity and availability). The matrix is not necessarily all-inclusive, but is intended to serve as a tool to assist in determining what features are required for each level of protection.

8.4. When individual security functions are used to support multiple security services and the level of protection required is not the same for each service, the security function will be implemented to support the highest level. For example, a mission support system processing unclassified information would require only the basic level for confidentiality, but the medium level for integrity and availability; in this case, the security function of access control would be implemented to support the medium level of protection.

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SERVICE	FUNCTION	BASIC	MEDIUM	HIGH
<b>Ref. Paragraph 4.1.3 Five Properties of Information Assurance</b>				
C	Confidentiality	- Type 4 algorithm - COTS	<u>If sensitive or format sensitive:</u> - Type 3 algorithm or Type 2 product - NIST-approved methods	- Type 1 product - NSA-approved methods

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SERVICE	FUNCTION	BASIC	MEDIUM	HIGH
I	Integrity	<ul style="list-style-type: none"> <li>- The system employs mechanisms to protect the information residing on the system from unauthorized modification or destruction</li> <li>- Non-repudiation (commercial products)</li> <li>- Configuration management</li> </ul>	<ul style="list-style-type: none"> <li>- DoD PKI</li> </ul>	<ul style="list-style-type: none"> <li>- DoD PKI</li> </ul>
A	Availability	<ul style="list-style-type: none"> <li>- Provides a mechanism to support weekly software and data backup, with daily incrementals</li> <li>- Contingency plans</li> </ul>	<ul style="list-style-type: none"> <li>- Provides a mechanism to support daily software and data backup, with hourly incrementals</li> <li>- Provides a mechanism for controlling and managing consumption of memory</li> </ul>	<ul style="list-style-type: none"> <li>- Provides a mechanism that incorporates synchronization points and allows recovery after a system failure or other discontinuity without a security compromise</li> <li>- Off-site storage and processing capabilities</li> <li>- Quarterly contingency exercises</li> </ul>
C,I,A	Availability (System Integrity)	<ul style="list-style-type: none"> <li>- Employs anti-virus software</li> <li>- Security-related advisories (e.g., ASSIST) are followed as soon as possible</li> </ul>	<ul style="list-style-type: none"> <li>- Audits data integrity</li> </ul>	<ul style="list-style-type: none"> <li>- TBD</li> </ul>
C,I	Authenticity (Identification & Authentication)	<ul style="list-style-type: none"> <li>- User ID and password (minimum 8 position alpha/numeric) with a mandatory update plan (COTS software based)</li> </ul>	<ul style="list-style-type: none"> <li>- User-specific token-based random number-generating floppy disk or smart card (COTS business grade standards)</li> </ul>	<ul style="list-style-type: none"> <li>- NSA endorsed smart card</li> </ul>

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SERVICE	FUNCTION	BASIC	MEDIUM	HIGH
C,I,A	Authenticity (Network Access Control)	<ul style="list-style-type: none"> <li>- Enable “connection idle” disconnect features where available</li> <li>- Boundary protection products configured to deny unauthorized access to all protected network components</li> </ul>	<ul style="list-style-type: none"> <li>- Monitor activities of any “mobile IP” connections</li> <li>- Boundary protection products configurable to dynamically deny access to IP addresses based on anomalous behavior (e.g., network flooding)</li> <li>- Provides insulation to prevent unintended/unauthorized access by “back-end” users</li> </ul>	<ul style="list-style-type: none"> <li>- NSA-endorsed protection of the communications path</li> <li>- Boundary protection products configurable to selectively manage traffic priority based on host or network IP address</li> </ul>
C,I,A	Authenticity (System Access Control)	<ul style="list-style-type: none"> <li>- Displays an advisory warning about monitoring prior to initiating the system logon procedure</li> <li>- Supports a privilege mechanism</li> <li>- Provides or incorporates a mechanism to authorize users to access the system</li> <li>- Provides a mechanism to limits the privilege a user may obtain based on means of access or port of entry</li> <li>- Operating system has built-in protection to prevent the bypassing of security and the unauthorized access to data</li> <li>- System software restricts individual access to only the files/data for which the user is authorized</li> </ul>	<ul style="list-style-type: none"> <li>- Procedures and mechanisms to protect against threats from connected networks operating at a lower security level than the local subscriber environment</li> </ul>	<ul style="list-style-type: none"> <li>- No additional requirements</li> </ul>
	Non-repudiation	-TBD	-TBD	-TBD

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SER VICE	FUNCTION	BASIC	MEDIUM	HIGH
<b>Ref. Paragraph 4.2 Non-Technical Countermeasures</b>				
C,I,A	Connection Approval	<ul style="list-style-type: none"> <li>- All connections to other systems or networks are subject to a connection approval process</li> <li>- MOUs required for non-DISN interconnection</li> </ul>	- No additional requirements	- No additional requirements
C	Connections of Systems at Different Classification Levels -- SABI (Secret and Below Interoperability)	- No connections permitted	- All connections have been subjected to the SABI process to measure community risk prior to connection	- No additional requirements
C,I,A	Personnel	<ul style="list-style-type: none"> <li>- All personnel receive background checks/investigations commensurate with their system responsibilities</li> </ul>	- No additional requirements	- No additional requirements
C,I,A	Personnel Security Training and Certification	<ul style="list-style-type: none"> <li>- A security awareness training plan is in place and in use</li> <li>- Users receive awareness training commensurate with their respective roles</li> <li>- Key personnel (i.e., system administrators) are formally trained for their respective roles</li> </ul>	<ul style="list-style-type: none"> <li>- Users receive formal training commensurate with their respective roles</li> <li>- Key personnel (i.e., system administrators) are formally certified for their respective roles</li> </ul>	- No additional requirements

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SERVICE	FUNCTION	BASIC	MEDIUM	HIGH
C,I,A	Physical	- A log is maintained of all personnel who enter or leave the building after normal duty hours and indicates the specific work spaces accessed	- The level of control and protection is commensurate with the highest classification or sensitivity level of the data being processed or resident in the system -	- No additional requirements
C,I,A	Procedural Security	-TBD	-TBD	-TBD
<b>Ref. Paragraph 4.3 Technical Countermeasures</b>				
C,I,A	Emanations Security	- No requirement	- IAW NSTISSI No. 7000, "TEMPEST Countermeasures for Facilities (U)"	- No additional requirements
	Remote Access and Remote Management	-TBD	-TBD	-TBD
	Firewalls	-TBD	-TBD	-TBD
	Mobile Computing	-TBD	-TBD	-TBD
	Information System Infrastructure	-TBD	-TBD	-TBD
	Virus and Malicious Code Protection	-TBD	-TBD	-TBD
	Certificate Management	-TBD	-TBD	-TBD
<b>Ref. Paragraph 5. Implementation</b>				
C,I,A	Certification and Accreditation	- Systems have been certified IAW with DITSCAP - Systems are accredited or have an IATO	- No additional requirements	- No additional requirements

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SER VICE	FUNCTION	BASIC	MEDIUM	HIGH
<b>Ref. Paragraph 6. Operations</b>				
C,I,A	Standard Operating Procedures (Administrative)	<ul style="list-style-type: none"> <li>- Users are prohibited from installing freeware, shareware, or public software on the system without appropriate administrative and technical oversight</li> <li>- All items of hardware are adequately identified and an inventory is maintained</li> <li>- Hard disks are cleared of sensitive information before being submitted for servicing</li> <li>- System security documentation equips the security administrator to understand and optimize the operation of all security features of the system to satisfy the security policy</li> </ul>	<ul style="list-style-type: none"> <li>- Procedures for reliable review of human readable system output are appropriate for the operating environment and sensitivity of the data</li> <li>- All removable media are controlled at the sensitivity level of information on the media</li> </ul>	<ul style="list-style-type: none"> <li>- All media which were used to store classified or highly sensitive information are overwritten, declassified, or destroyed when no longer needed</li> <li>- Positive security controls are maintained over all components of a system at all times</li> </ul>
	Access	-TBD	-TBD	-TBD
	Use of PKI Certificates	-TBD	-TBD	-TBD
A	Contingency Planning	<ul style="list-style-type: none"> <li>- A contingency plan exists which covers all anticipated emergency situations, backups, and disaster recovery</li> </ul>	<ul style="list-style-type: none"> <li>- The contingency plan clearly outlines the amount of downtime that can be tolerated</li> </ul>	<ul style="list-style-type: none"> <li>- The contingency plan is tested at least annually</li> </ul>
I,A	Security Incident Procedures (Event Detection and Countermeasures)	<ul style="list-style-type: none"> <li>- Controls exist to detect and/or prevent covert penetration attempts</li> <li>- Capability to identify and record unauthorized attempts to gain access</li> </ul>	<ul style="list-style-type: none"> <li>- No additional requirements</li> </ul>	<ul style="list-style-type: none"> <li>- No additional requirements</li> </ul>

SECURITY		LEVEL OF PROTECTION REQUIREMENTS ARE ADDITIVE FROM LEFT TO RIGHT		
SER VICE	FUNCTION	BASIC	MEDIUM	HIGH
I,A	Security Incident Procedures (Incident and Vulnerability Reporting)	- Per JTF-CND direction	- No additional requirements	- No additional requirements
<b>Ref. Paragraph 7. System Management</b>				
	Configuration Management			
C	Data Management (Labels and Marking)	- No data is introduced into the system without designation of the sensitivity of the data - Classified and sensitive unclassified output, containers, and media are marked in accordance with DoD requirements	- No data is introduced into the system without designation of the classification or sensitivity of the data; e.g., text markings on soft copies (documents, presentations, etc.) and fields in databases	- Provides security parameters, sensitivity labels, and information labels for the information it stores and processes and for the information it exchanges with other system
	Password Management	- TBD	- TBD	- TBD
C,I,A	Audit (Network)	- TBD	- TBD	- TBD

**Part III -- References**

- (a) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
- (b) DoD 5200.28-M, "ADP Security Manual," January 1973 and Change 1, June 24, 1979
- (c) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990
- (d) DCIS No1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Systems and Networks (U)," 19 July, 1988
- (e) SM-313-83, "Safeguarding the Single Integrated Operational Plan (U)," May 10, 1983
- (f) DoD Directive O-5205.7 "Special Access Program (SAP) Policy," January 13, 1997.
- (g) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," August 1997
- (h) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 23, 1998
- (i) Title 10, United States Code
- (j) Public Law 100-235, "The Computer Security Act of 1987," as amended, January 8, 1988
- (k) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process," December 30, 1997
- (l) DoD Regulation 5200.2R, "Personnel Security Program," May 6, 1992
- (m) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Secret and Below Interoperability (SABI)," March 20, 1997
- (n) Deputy Secretary of Defense Policy Memorandum, "Web Site Administration," December 7, 1998.
- (o) DoD Directive 4640.6, "Communications Security (COMSEC) Monitoring and Recording," June 26, 1981
- (p) PKI guidance TBD
- (q) Under Secretary of Defense (Personnel and Readiness) and Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Joint Memorandum, "Information Assurance (IA) Training and Certification," June 29, 1998
- (r) Presidential Decision Directive/NSC -63, Subject: "Critical Infrastructure Protection," May 22, 1998
- (s) National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 503, "Incident Response and Vulnerability Reporting for National Security Systems," August 30, 1993



## Part IV -- Definitions

1. **Community Risk**. A combination of: 1) the likelihood that a threat will occur within an interacting population; 2) the likelihood that a threat occurrence will result in an adverse impact to some or all members of that populace; and 3) the severity of the resulting impact. (SABI Terms of Reference (TOR))
2. **Connection Approval**. Authorization to link or join a system with an existing network. (SABI TOR)
3. **Criticality**. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing. (SABI Handbook)
4. **Defense Information Infrastructure (DII)**. Information transfer and processing resources, including information and data storage, manipulation, retrieval, and display; the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structure serving the DoD's local and worldwide information needs. The DII connects DoD mission, support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and provides information processing and value-added services to subscribers over the Defense Information Systems Network (DISN). The DII is comprised of DoD-wide elements and Component-specific elements (i.e., sustaining base, tactical, C4I interfaces to weapon systems). Unique user data, information, and user applications software are not considered part of the DII. Information systems that support functions, which require open, uncontrolled access (i.e., web servers for official home page information intended for dissemination to the general public) are not considered part of the DII and are isolated from it. (DoDI 5200.40, DITSCAP, modified)
5. **DoD Information Technology Security Certification and Accreditation Process (DITSCAP)**. The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (DoDI 5200.40)
6. **Format Sensitive Information**. Unclassified information regarding DoD capabilities, infrastructure, personnel and/or operational procedures which, when electronically aggregated in significant volume, could adversely affect the national interest, the conduct of federal programs, or the privacy of individuals if lost, misused, accessed, or modified in an unauthorized way, is format sensitive information. Includes information that may be subject to public disclosure but requires protection when in electronic format.

7. **Functional Domain.** An identifiable DoD functional mission area. For purposes of this policy memorandum, the functional domains are: command and control, logistics, transportation, health affairs, intelligence, personnel, financial services, and research and development.
8. **Incident and Detection Response Capabilities.** The establishment of mechanisms and procedures to monitor information systems and networks; detect, report and document attempted or realized penetrations of those systems and networks; and institute appropriate countermeasures or corrective actions.
9. **Information Assurance.** Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD S-3600.1)
10. **Information Operation Condition (INFOCON).** The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack); BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions
11. **Information Owner.** The organization which creates and is responsible for managing specific information. Usually the principal user of the information created.
12. **Information System.** The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information. (NSTISSI 4009)
13. **Infrastructure.** The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, or society as a whole. [DoDD 5160.54, Critical Asset Assurance Program (CAAP)]
14. **Layered Defense.** A combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection.
15. **Level of Protection.** The extent to which protective measures, techniques and procedures must be applied to information systems. DoD has three levels of protection:

- a. **Basic**: Information systems which require implementation of the DoD standard minimum security countermeasures.
- b. **Medium**: Information systems which require layering of additional safeguards above the DoD standard minimum security countermeasures.
- c. **High**: Information systems which require the most stringent protection and rigorous security countermeasures

16. **Mission Category**. Applicable to information systems, the category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. DoD will have three categories:

- a. **Mission Critical**. Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information).

- b. **Mission Support**. Systems handling information that is important to the support of deployed and contingency forces; must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

- c. **Administrative**. Systems handling information which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

17. **Network Centric**. A holistic view of interconnected information systems and resources that encourages a broader approach to security management than a component-based approach. (SABI TOR)

18. **Operating Environment**. The total environment in which an information system operates. Includes the physical facility and controls, procedural and administrative controls, personnel controls (e.g., clearance level of the least cleared user).

19. **Public Key Infrastructure (PKI)**. An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

20. **Secret and Below Interoperability (SABI) Initiative**. An ASD (C3I) directed, JCS sponsored, NSA/DISA executed initiative to enhance Secret and Below Interoperability, measure community risk, and protect the GNIE. (SABI Handbook)

